

May 18, 2021

CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT TACOMA
BY _____ DEPUTY

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Digital Devices more fully described in Attachment A

Case No. MJ21-5105

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Digital Devices, more fully described in Attachment A, incorporated herein by reference.

located in the _____ Western _____ District of _____ Washington _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. § 7, 2441(c), & 2246 Aggravated Sexual Abuse of a Minor
 18 U.S.C. § 2251(a), (e) Production of Child Pornography
 18 U.S.C. § 2252(a)(4)(B), (b)(2) Possession of Child Pornography

The application is based on these facts:

- ☒ See Affidavit of FBI Special Agent Kelsey Mendoza, attached hereto and incorporated herein by reference.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Kelsey M. Mendoza
 Applicant's signature

KELSEY M. MENDOZA, Special Agent, FBI

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 05/18/2021

David W. Christel
 Judge's signature

City and state: Tacoma, Washington

DAVID W. CHRISTEL, United States Magistrate Judge

Printed name and title

1 turned over by victim's relative on April 30, 2021, to the FBI, including two WD
2 Passports (External Hard Drives), one Dell laptop, one Apple iPhone, and 10 flash drives,
3 currently in the custody of the FBI.

4 4. As set forth below, there is probable cause to believe that the SUBJECT
5 ITEMS will contain or possess evidence, fruits, and instrumentalities of violations of 18
6 U.S.C. §§ 7, 2241(c), and 2246 (Aggravated Sexual Abuse of a Minor), 18 U.S.C.
7 § 2251(a), (e) (Production of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B), (b)(2)
8 (Possession of Child Pornography), as well as attempt or conspiracy to commit such
9 offenses (hereinafter the "TARGET OFFENSES"). I seek authorization to search and
10 seize the items specified in Attachment B, which is incorporated herein by reference.

11 5. The information in this affidavit is based upon the investigation I have
12 conducted in this case, my conversations with other law enforcement officers who have
13 engaged in various aspects of this investigation, and my review of reports written by
14 other law enforcement officers involved in this investigation.

15 6. Because this affidavit is being submitted for the limited purpose of securing
16 search warrants, I have not included each and every fact known to me concerning this
17 investigation. I have set forth only those facts that I believe are sufficient to establish
18 probable cause to support the issuance of the requested warrants.

19 7. This Affidavit is being presented electronically pursuant to Local Criminal
20 Rule CrR 41(d)(3).

21 **III. SUMMARY OF THE INVESTIGATION**

22 8. This investigation arose from a report received by the Criminal
23 Investigation Division Command (CID) located on Joint Base Lewis-McChord, WA.
24 The reporting party, who has a close relationship to the minor victim (MV), stated that
25 JOSHUA HARROD, had sexually abused MV. MV whose identity should be protected,
26 is currently under the age of 13. At the time of the abuse, MV was approximately 8 years
27 old.
28

1 9. HARROD is a former Special Agent within the United States Air Force,
2 Office of Special Investigations. He was separated from the U.S. Air Force in 2018 and
3 currently serves in the Army National Guard as a Recruiter.

4 10. On November 6, 2020 and March 2021, MV participated in a forensic
5 interview, which was conducted by the Federal Bureau of Investigation's Child and
6 Adolescent Forensic Interviewer, Erin Lehto. During the interviews, MV stated the acts
7 of physical and sexual abuse occurred on Joint Base Lewis-McChord while HARROD
8 was still on active duty in the United States Air Force.

9 11. According to Erica Harrod (Pheiler), his former spouse, HARROD resided
10 in a trailer on post beginning around October 2017. The trailer was parked in a long-term
11 camping site, located on the federally owned government property of the JBLM military
12 installation. The abuse occurred at HARROD's residence. HARROD completed duties
13 at JBLM and his active-duty service on or before April 20, 2018.

14 12. On multiple occasions, HARROD sexually abused MV while she was in his
15 custody and care. MV stated that all the physical abuse occurred at HARROD's JBLM
16 residence. MV described digital, anal and tongue penetration all committed by the
17 SUBJECT. MV stated that the penetration began approximately one month after she
18 began visiting HARROD without supervision.

19 13. MV recalled one instance where the HARROD told her to lie on her
20 stomach, "that she would like it." He covered his penis with an "elastic" and then
21 penetrated her anus. She remembered telling her mom that she was constipated, and that
22 was why she was bleeding from her buttocks. During another instance, she said that his
23 penis "sweated" clear liquid, normally going on the bed, but once he made her lick his
24 penis and the liquid went into her mouth.

25 14. HARROD penetrated her anus and vagina with his tongue. He would
26 instruct MV to get into a crawling position and he would then penetrate her using his
27 tongue, moving it in a circular motion. Lastly, on one occasion while in public,
28 HARROD put his hands down MV's pants and digitally penetrated her anus.

1 15. HARROD also sexually abused her while taking a shower in the communal
2 shower area located near his trailer. She recalled that he would say that her hair still had
3 conditioner in it. He would send her little sister back to the trailer while he helped her
4 rewash her hair. HARROD would go into the same shower stall as MV and rub her hair
5 as if getting the conditioner out. MV stated that he would say that he forgot to wash
6 himself and asked if she could help. While she used a bar of soap to wash his body, he
7 would run his fingers through her hair. She noticed that while she washed him, his penis
8 became erect. Once she finished washing him, he would take the bar of soap, lather his
9 hands up, and then wash her body. He would start at the top and work his way down her
10 body. MV recalled him spending a lot of time rubbing her chest area and nipples. He
11 also penetrated her vagina with his fingers which she said was very uncomfortable and
12 would cause irritation to her vaginal area. While inside, his fingers would move back and
13 forth causing her vagina to throb but also feel good.

14 16. In addition to touching and penetrating her vagina, HARROD would grab
15 her buttocks and would touch her anus. When he did, he would make circular motions
16 around her anus with his fingers.

17 17. MV disclosed that HARROD would insist that she lay down and
18 sleep/cuddle with him. While lying on the bed with him, and during other occasions, he
19 would inch his way over towards MV until his penis touched her back, stomach or
20 vagina. He would also ask her to cuddle while he laid on his back. This would result in
21 her lying on top of him, stomach to stomach. His penis would either be touching her
22 vagina or stomach. She described his penis as getting hard and "it was like lying on a
23 rock".

24 18. She recalled a separate instance when they were lying down on the bed
25 facing each other, where he asked her to hold his penis. At the time he asked, his penis
26 was touching her stomach. While she held his penis in her open palm, he was grabbing
27 her buttocks. She stated that the bed got wet and that his penis was 'sweating'.
28

1 19. She had felt the ‘wet’ multiple times. One occasion described above, she
2 was holding his penis and the bed felt wet afterwards. During another incident,
3 HARROD put his penis inside of her vagina, his body would twitch, and then his penis
4 tensed up. HARROD’s hands were grabbing her butt, and she then felt the ‘wet’. The
5 third instance was when HARROD used his penis to go in circular motions around her
6 vagina. He then ejaculated inside her vagina. Lastly, he would put his penis between her
7 buttocks. MV was facing away from him, she described his penis getting stiff and then
8 soft. She recalled him moving his body back and forth and then she felt the ‘wet’ running
9 down her leg.

10 20. MV stated that HARROD would be on the phone a lot. She recalled one
11 instance while she was undressing, HARROD took a photo of her. She explained that
12 she had asked what he was doing, and he said that he was on his Facebook, but MV
13 remembers hearing “the photo noise.”

14 21. HARROD threatened MV that there would be consequences if she told
15 anyone about what was occurring and he also threatened to kill her mother if anyone
16 found out. Additionally, he would physically abuse MV such that he caused her to wear
17 long sleeves to hide the bruising.

18 22. While married to Erica Pheiler, HARROD periodically obtained and used
19 various digital devices to store data including pictures and videos. Pheiler possessed
20 greater technological understanding of and experience with digital devices. Accordingly,
21 HARROD often asked Pheiler to diagnose and resolve any technological issues he
22 experienced with his digital devices.

23 23. Between the years of 2012 and 2015, HARROD asked Pheiler to assist him
24 with a digital device, specifically a black laptop. While reviewing said device, Pheiler
25 observed certain files featuring file names that contained words to the effect of “Father,
26 Daughter.” Pheiler, although she suspected these files contained child pornography, did
27 not access the images/videos. When she confronted HARROD about the files, he said “if
28 you watch it, she definitely isn’t a child.”

24. In June 2017, Pheiler legally divorced HARROD. HARROD transferred to an installation in Kocaeli, Turkey, and had his household goods shipped from the residence that he shared with Pheiler to Turkey. He resided in Turkey from July 2015 until approximately October 2016. At the time he departed, he left, in her custody and care, the following digital devices: two WD Passports, one Dell laptop, one Apple iPhone, and 10 flash drives. On April 30, 2021, Pheiler transferred the SUBJECT ITEMS to the FBI and provided written consent for examination.

25. The Island County Sheriff's Office interviewed Pheiler in March 2020, when she was accused of abusing Harrod. LE conducted a forensic exam of her personal cell phone, which they returned the same day and reviewed some, but not all, of the other devices. However, when a copy of the forensic examinations and report was requested, LE stated the files had been purged.

26. Since 2015, HARROD had not inquired about the SUBJECT ITEMS or sought their return. Pheiler had continuous access to the SUBJECT ITEMS and did not believe that any one of the devices had restricted or password protected access. On April 7, 2021, a Washington State Patrol Detective from the High Technology Crimes Unit created a forensic image of the SUBJECT ITEMS but has not undertaken further review of the forensic images pending the instant search warrant application.¹

IV. BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

27. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

¹ The Government reserves the legal position that the SUBJECT ITEMS are lawfully within its possession and, in part based upon Pheiler's continuing consent to search, may be lawfully searched. Notwithstanding this position, the Government is nevertheless pursuing the instant application for a search warrant out of an abundance of caution.

1 b. Computers and digital technology are the primary way in which
2 individuals interested in child pornography interact with each other. Computers basically
3 serve four functions in connection with child pornography: production, communication,
4 distribution, and storage.

5 c. Digital cameras and smartphones with cameras save photographs or
6 videos as a digital file that can be directly transferred to a computer by connecting the
7 camera or smartphone to the computer, using a cable or via wireless connections such as
8 “Wi-Fi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may
9 be stored on a removable memory card in the camera or smartphone. These memory
10 cards are often large enough to store thousands of high-resolution photographs or videos.

11 d. A device known as a modem allows any computer to connect to
12 another computer through the use of telephone, cable, or wireless connection. Mobile
13 devices such as smartphones and tablet computers may also connect to other computers
14 via wireless connections. Electronic contact can be made to literally millions of
15 computers around the world. Child pornography can therefore be easily, inexpensively
16 and anonymously (through electronic communications) produced, distributed, and
17 received by anyone with access to a computer or smartphone.

18 e. The computer’s ability to store images in digital form makes the
19 computer itself an ideal repository for child pornography. Electronic storage media of
20 various types - to include computer hard drives, external hard drives, CDs, DVDs, and
21 “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a
22 port on the computer - can store thousands of images or videos at very high resolution. It
23 is extremely easy for an individual to take a photo or a video with a digital camera or
24 camera-bearing smartphone, upload that photo or video to a computer, and then copy it
25 (or any other files on the computer) to any one of those media storage devices. Some
26 media storage devices can easily be concealed and carried on an individual’s person.
27 Smartphones and/or mobile phones are also often carried on an individual’s person.
28

1 f. The Internet affords individuals several different venues for
2 obtaining, viewing, and trading child pornography in a relatively secure and anonymous
3 fashion.

4 g. Individuals also use online resources to retrieve and store child
5 pornography. Some online services allow a user to set up an account with a remote
6 computing service that may provide email services and/or electronic storage of computer
7 files in any variety of formats. A user can set up an online storage account (sometimes
8 referred to as “cloud” storage) from any computer or smartphone with access to the
9 Internet. Even in cases where online storage is used, however, evidence of child
10 pornography can be found on the user’s computer, smartphone, or external media in most
11 cases.

12 h. A growing phenomenon related to smartphones and other mobile
13 computing devices is the use of mobile applications, also referred to as “apps.” Apps
14 consist of software downloaded onto mobile devices that enable users to perform a
15 variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or
16 playing a game – on a mobile device. Individuals commonly use such apps to receive,
17 store, distribute, and advertise child pornography, to interact directly with other like-
18 minded offenders or with potential minor victims, and to access cloud-storage services
19 where child pornography may be stored.

20 i. As is the case with most digital technology, communications by way
21 of computer can be saved or stored on the computer used for these purposes. Storing this
22 information can be intentional (i.e., by saving an email as a file on the computer or saving
23 the location of one’s favorite websites in, for example, “bookmarked” files) or
24 unintentional. Digital information, such as the traces of the path of an electronic
25 communication, may also be automatically stored in many places (e.g., temporary files or
26 ISP client software, among others). In addition to electronic communications, a
27 computer user’s Internet activities generally leave traces or “footprints” in the web cache
28

1 and history files of the browser used. Such information is often maintained indefinitely
2 until overwritten by other

3 28. Based upon my knowledge, experience, and training in child pornography
4 investigations, and the training and experience of other law enforcement officers with
5 whom I have had discussions, I know that there are certain characteristics common to
6 individuals who have a sexualized interest in children and depictions of children:

7 a. They may receive sexual gratification, stimulation, and satisfaction
8 from contact with children; or from fantasies they may have viewing children engaged in
9 sexual activity or in sexually suggestive poses, such as in person, in photographs, or other
10 visual media; or from literature describing such activity.

11 b. They may collect sexually explicit or suggestive materials in a
12 variety of media, including photographs, magazines, motion pictures, videotapes, books,
13 slides, and/or drawings or other visual media. Such individuals often times use these
14 materials for their own sexual arousal and gratification. Further, they may use these
15 materials to lower the inhibitions of children they are attempting to seduce, to arouse the
16 selected child partner, or to demonstrate the desired sexual acts. These individuals may
17 keep records, to include names, contact information, and/or dates of these interactions, of
18 the children they have attempted to seduce, arouse, or with whom they have engaged in
19 the desired sexual acts.

20 c. They often maintain any “hard copies” of child pornographic
21 material that is, their pictures, films, video tapes, magazines, negatives, photographs,
22 correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of
23 their home or some other secure location. These individuals typically retain these “hard
24 copies” of child pornographic material for many years, as they are highly valued.

25 d. Likewise, they often maintain their child pornography collections
26 that are in a digital or electronic format in a safe, secure and private environment, such as
27 a computer and surrounding area. These collections are often maintained for several
28

1 years and are kept close by, often at the individual's residence or some otherwise easily
2 accessible location, to enable the owner to view the collection, which is valued highly.

3 e. They also may correspond with and/or meet others to share
4 information and materials; rarely destroy correspondence from other child pornography
5 distributors/collectors; conceal such correspondence as they do their sexually explicit
6 material; and often maintain lists of names, addresses, and telephone numbers of
7 individuals with whom they have been in contact and who share the same interests in
8 child pornography.

9 f. They generally prefer not to be without their child pornography for
10 any prolonged time period. This behavior has been documented by law enforcement
11 officers involved in the investigation of child pornography throughout the world.
12 Importantly, e-mail and cloud storage can be a convenient means by which individuals
13 can access a collection of child pornography from any computer, at any location with
14 Internet access. Such individuals therefore do not need to physically carry their
15 collections with them but rather can access them electronically. Furthermore, these
16 collections can be stored on email "cloud" servers, which allow users to store a large
17 amount of material at no cost, without leaving any physical evidence on the users'
18 computer(s).

19 29. Even if such individuals use a portable device (such as a mobile phone) to
20 access the Internet and child pornography, it is more likely than not that evidence of this
21 access will be found in their home, including on digital devices other than the portable
22 device (for reasons including the frequency of "backing up" or "synching" mobile phones
23 to computers or other digital devices).

24 30. In addition to offenders who collect and store child pornography, law
25 enforcement has encountered offenders who obtain child pornography from the internet,
26 view the contents and subsequently delete the contraband, often after engaging in self-
27 gratification. In light of technological advancements, increasing Internet speeds and
28 worldwide availability of child sexual exploitative material, this phenomenon offers the

1 offender a sense of decreasing risk of being identified and/or apprehended with quantities
2 of contraband. This type of consumer is commonly referred to as a ‘seek and delete’
3 offender, knowing that the same or different contraband satisfying their interests remain
4 easily discoverable and accessible online for future viewing and self-gratification. I
5 know that, regardless of whether a person discards or collects child pornography he/she
6 accesses for purposes of viewing and sexual gratification, evidence of such activity is
7 likely to be found on computers and related digital devices, including storage media, used
8 by the person. This evidence may include the files themselves, logs of account access
9 events, contact lists of others engaged in trafficking of child pornography, backup files,
10 and other electronic artifacts that may be forensically recoverable.

11 31. Given the above-stated facts, including the victim’s description of child
12 sexual abuse and HARROD’s use of his phone and the fact that HARROD is not believed
13 to be aware of the investigation against him, and based on my knowledge, training and
14 experience, along with my discussions with other law enforcement officers who
15 investigate child exploitation crimes, I believe that HARROD likely has a sexualized
16 interest in children and depictions of children and that evidence of child pornography is
17 likely to be found on the SUBJECT ITEMS.

18 **V. FRUITS, EVIDENCE, AND INSTRUMENTALITIES STORED ON**
19 **ELECTRONIC DEVICES**

20 32. As described above and in Attachment B, this application seeks permission
21 to search for and seize items listed in Attachment B that might be found on the SUBJECT
22 ITEMS, in whatever form they are found. One form in which evidence, fruits, or
23 instrumentalities might be found is data stored on a computer’s hard drive or other digital
24 device or electronic storage media. Thus, the warrants applied for would authorize the
25 search and seizure of electronic storage media or, potentially, the copying of
26 electronically stored information, all under Rule 41(e)(2)(B).
27
28

1 33. *Probable cause.* Based upon my review of the evidence gathered in this
2 investigation, my review of data and records, information received from other agents and
3 computer forensic examiners, and my training and experience, there is probable cause to
4 believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES will be
5 stored on those SUBJECT ITEMS. As noted above, my investigation has shown that
6 JOSHUA HARROD likely used a cell phone and/or camera to record the sexual abuse of
7 a minor. Furthermore, my investigation has revealed the presence of digital files on one
8 or more of the SUBJECT ITEMS bearing titles associated with sexually explicit images
9 of children. There is, therefore, probable cause to believe that evidence, fruits, and
10 instrumentalities, of the crimes under investigation exist and will be found on the
11 SUBJECT ITEMS for at least the following reasons:

12 a. Based my knowledge, training, and experience, I know that
13 computer files or remnants of such files may be recovered months or even years after
14 they have been downloaded onto a storage medium, deleted, or viewed via the Internet.
15 Electronic files downloaded to a storage medium can be stored for years at little or no
16 cost. Even when files have been deleted, this information can sometimes be recovered
17 months or years later with forensics tools. This is because when a person “deletes” a file
18 on a computer, the data contained in the files does not actually disappear; rather, that data
19 remains on the storage medium until it is overwritten by new data.

20 b. Therefore, deleted files, or remnants of deleted files, may reside in
21 free space or slack space—that is, in space on the storage medium that is not currently
22 being used by an active file—for long periods of time before they are overwritten. In
23 addition, a computer’s operating system may also keep a record of deleted data in “swap”
24 or “recovery” files.

25 c. Wholly apart from user-generated files, computer storage media—in
26 particular, computers’ internal hard drives—contain electronic evidence of how a
27 computer has been used, what is has been used for, and who has used it. To give a few
28 examples, this forensic evidence can take the form of operating system configurations,

1 artifacts from operating system or application operation, file system data structures, and
2 virtual memory “swap” paging files. Computer users typically do not erase or delete this
3 evidence, because special software is typically required for that task. However, it is
4 technically possible to delete this information.

5 d. Similarly, files that have been viewed via the Internet are sometimes
6 automatically downloaded into a temporary Internet directory or “cache.”

7 e. Digital storage devices may also be large in capacity, but small in
8 physical size. Because those who are in possession of such devices also tend to keep
9 them on their persons, especially when they may contain evidence of a crime. Digital
10 storage devices may be smaller than a postal stamp in size, and thus they may easily be
11 hidden in a person’s pocket.

12 34. Searching computer systems is a highly technical process that requires
13 specific expertise and specialized equipment. There are so many types of computer
14 hardware and software in use today that it is rarely possible to bring to the search site all
15 the necessary technical manuals and specialized equipment necessary to consult with
16 computer personnel who have expertise in the type of computer, operating system, or
17 software application being searched.

18 35. The analysis of computer systems and storage media often relies on
19 rigorous procedures designed to maintain the integrity of the evidence and to recover
20 “hidden,” mislabeled, deceptively named, erased, compressed, encrypted or password-
21 protected data, while reducing the likelihood of inadvertent or intentional loss or
22 modification of data. A controlled environment such as a laboratory, is typically required
23 to conduct such an analysis properly.

24 36. The volume of data stored on many computer systems and storage devices
25 will typically be so large that it will be highly impracticable to search for data during the
26 execution of the physical search of the premises. The hard drives commonly included in
27 desktop and laptop computers are capable of storing millions of pages of text.
28

1 37. A search of digital devices for evidence described in Attachment B may
2 require a range of data analysis techniques. In some cases, agents may recover evidence
3 with carefully targeted searches to locate evidence without requirement of a manual
4 search through unrelated materials that may be commingled with criminal evidence.
5 Agents may be able to execute a “keyword” search that searches through the files stored
6 in a digital device for special terms that appear only in the materials covered by the
7 warrant. Or, agents may be able to locate the materials covered by looking for a
8 particular directory or name. However, in other cases, such techniques may not yield the
9 evidence described in the warrant. Individuals may mislabel or hide files and directories;
10 encode communications to avoid using keywords; attempt to delete files to evade
11 detection; or take other steps designed to hide information from law enforcement
12 searches for information.

13 38. The search procedure of any digital device seized may include the
14 following on-site techniques to seize the evidence authorized in Attachment B:

15 a. On-site triage of computer systems to determine what, if any,
16 peripheral devices or digital storage units have been connected to such computer systems,
17 a preliminary scan of image files contained on such systems and digital storage devices to
18 help identify any other relevant evidence or co-conspirators.

19 b. On-site copying and analysis of volatile memory, which is usually
20 lost if a computer is powered down, and may contain information about how the
21 computer is being used, by whom, when and may contain information about encryption,
22 virtual machines, or steganography which will be lost if the computer is powered down.

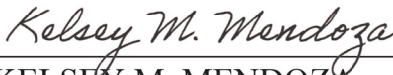
23 c. On-site forensic imaging of any computers may be necessary for
24 computers or devices that may be partially or fully encrypted in order to preserve
25 unencrypted data that may, if not immediately imaged on-scene become encrypted and
26 accordingly become unavailable for any examination.

27 39. *Nature of examination.* Based on the foregoing, and consistent with Rule
28 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise

1 copying storage media that reasonably appear to contain some or all of the evidence
2 described in the warrant, and would authorize a later review of the media or information
3 consistent with the warrant. The later review may require techniques, including but not
4 limited to computer-assisted scans of the entire medium, including encrypted partitions,
5 that might expose many parts of a hard drive to human inspection in order to determine
6 whether it is evidence described by the warrant.

7 VI. CONCLUSION

8 40. Based on the information set forth herein, there is probable cause to search
9 the above described SUBJECT ITEMS, as further described in Attachment A, as well as
10 on and in any digital device or other electronic storage media found therein or thereon,
11 for evidence, fruits and instrumentalities, as further described in Attachment B, of the
12 TARGET OFFENSES.

13
14 
15 _____
16 KELSEY M. MENDOZA
17 Special Agent, FBI

18 The above-named agent provided a sworn statement attesting to the truth of the
19 foregoing Affidavit submitted to me by reliable electronic means pursuant to Fed. R.
20 Crim. Proc. 4.1(a) on this 18th day of May, 2021.

21
22 
23 _____
24 DAVID W. CHRISTEL
25 United States Chief Magistrate Judge
26
27
28

ATTACHMENT A

Description of Property to be Searched

Digital devices (SUBJECT ITEMS) turned over by victim's relative on April 30, 2021, to the FBI, including: two WD Passports (External Hard Drives), one Dell laptop, one Apple iPhone, and 10 flash drives.

ATTACHMENT B**ITEMS TO BE SEIZED**

Evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 7, 2241(c), and 2246 (Aggravated Sexual Abuse of a Minor), 18 U.S.C. § 2251(a), (e) (Production of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B), (b)(2) (Possession of Child Pornography), as well as attempt or conspiracy to commit such offenses committed in or after October 2017, as follows:

- a. Items, records, or information² relating to visual depictions of minors engaged in sexually explicit conduct;
- b. Items, records, or information, including photos, bedding, or personal effects, that might corroborate allegations of sexual abuse by MV or suggest a sexualized interest in MV or other minors;
- c. Items, records, or information relating to the identity of the creator(s) of or subject(s) depicted in any visual depiction of a minor engaged in sexually explicit conduct;
- d. Items, records, or information relating to the location of or circumstances surrounding the creation of any visual depiction of a minor engaged in sexually explicit conduct;
- e. Items, records, or information relating to the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;
- f. Items, records, or information concerning communications about the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct;

² As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

- g. Items, records, or information concerning communications about the sexual abuse or exploitation of minors;
- h. Items, records, or information related to communications with or about minors;
- i. Items, records, or information concerning the identities and contact information (including mailing addresses) of any individuals involved in the receipt, distribution, or transportation of visual depictions of minors engaged in sexually explicit conduct, saved in any form;
- j. Items, records, or information concerning occupancy, residency or ownership of the SUBJECT PREMISES, including without limitation, utility and telephone bills, mail envelopes, addressed correspondence, purchase or lease agreements, diaries, statements, identification documents, address books, telephone directories, and keys;
- k. Items, records, or information concerning the ownership or use of computer equipment found in the SUBJECT PREMISES, including, but not limited to, sales receipts, bills for internet access, handwritten notes, and computer manuals;
- l. Any digital devices or other electronic storage media³ and/or their components including:
 - i. any digital device or other electronic storage media capable of being used to commit, further, or store evidence, fruits, or instrumentalities of the offenses listed above;
 - ii. any magnetic, electronic or optical storage device capable of storing data, including thumb drives, SD cards, or external hard drives;

³ The term “digital devices” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware. The term “electronic storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

- 1 iii. any physical keys, encryption devices, dongles and similar physical
- 2 items that are necessary to gain access to the computer equipment,
- 3 storage devices or data; and
- 4 iv. any passwords, password files, test keys, encryption codes or other
- 5 information necessary to access the computer equipment, storage
- 6 devices or data.
- 7 m. For any digital device or other electronic storage media whose seizure is
- 8 otherwise authorized by this warrant, and any digital device or other
- 9 electronic storage media that contains or in which is stored records or
- 10 information that is otherwise called for by this warrant:
- 11 i. evidence of who used, owned, or controlled the digital device or
- 12 other electronic storage media at the time the things described in this
- 13 warrant were created, edited, or deleted, such as logs, registry
- 14 entries, configuration files, saved usernames and passwords,
- 15 documents, browsing history, user profiles, email, email contacts,
- 16 “chat,” instant messaging logs, photographs, and correspondence;
- 17 ii. evidence of software that would allow others to control the digital
- 18 device or other electronic storage media, such as viruses, Trojan
- 19 horses, and other forms of malicious software, as well as evidence of
- 20 the presence or absence of security software designed to detect
- 21 malicious software;
- 22 iii. evidence of the lack of such malicious software;
- 23 iv. evidence of the attachment to the digital device of other storage
- 24 devices or similar containers for electronic evidence;
- 25 v. evidence of counter-forensic programs (and associated data) that are
- 26 designed to eliminate data from the digital device or other electronic
- 27 storage media;
- 28 vi. evidence of the times the digital device or other electronic storage
- media was used;
- vii. passwords, encryption keys, and other access devices that may be
- necessary to access the digital device or other electronic storage
- media;

- viii. documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;
- ix. records of or information about the Internet Protocol used by the digital device or other electronic storage media;
- x. records of internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any internet search engine, and records of user-typed web addresses.
- xi. contextual information necessary to understand the evidence described in this attachment.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES.